基于科斯定律的开放数据平台地理位置隐私保护对策研究[1)]

王树义　吴查科
（天津师范大学管理学院 天津 300387）

摘要　本文基于科斯定律，结合大数据 3V 特性生成综合分析框架，寻找地理位置隐私信息泄露的主要责任方。利用数据挖掘、数据可视化和影子分析等研究方法，本研究以合法手段尝试获取开放数据集合中社交媒体平台用户地理位置信息，以测试现有隐私保护方案的漏洞，并寻找保护地理位置隐私的最小代价有效方案。在科斯定律的分析框架下，本文认定了地理位置隐私泄露的主要责任方，并根据隐私泄露的方式有的放矢地提出了相应对策。

关键词　隐私保护　地理位置　开放数据

Countermeasure Study of Open Data Location Privacy Protection Based on Coase Theorem

Wang Shuyi and Wu Chake
(Management School, Tianjin Normal University, Tianjin 300387, China)

Abstract　Based on a comprehensive analytical framework generated by Coase theorem and three Big Data properties, this paper searched for the main liable actor who should be responsible for leakage of geo location privacy. Data mining, data visualization and shadowing analysis were adopted to gather social media user location information legally from open data platform. It was used to test the vulnerability of existing privacy protection mechanisms and seek the effective solution of the minimum cost for geo location privacy protection. In the above framework, the main liable actor was decided and a particular countermeasure was proposed.

Keywords　privacy protection, geo location, open data

1 引　言

日益发展的大数据分析技术如同一把双刃剑，在给人们带来了便捷、效率与个性化体验的同时，也威胁着用户隐私信息的安全[1]。移动社交媒体运营商、公用事业机构与政府网站都在大规模开放原始数据[2,3]。数据开放的趋势使得隐私泄露的威胁逐渐加大。已有的案例证明了地理位置信息遭到泄露之后的结果非常严重[4]。2010 年 2 月，新上线的网站“Please rob me”根据人们在 Foursquare 应用上面的签到信息推测出哪些人不在家中，给了盗贼十足的可乘之机[5]。用户的签到行为让许多跟踪狂(stalker)异常欣喜，他们利用 Foursquare 设计的 API 对某个设定区域内的女性用户进行定位，搜寻潜在的受害者。2012 年 5 月，Foursquare 网站不得不关闭了相应的 API 数据调用功能[6]。

开放数据引发的地理位置信息泄露问题曾经被许多研究者关注过，并提出了若干种对策[7-11]。然而经过本课题组对相关文献的梳理，尚未发现有效的用户地理位置保护方案。我们依据文献的回顾，主要归结为以下两方面的原因：

一是大数据的特性更为复杂。大数据具有容量大（volume）、速度快（velocity）和种类多（variety）的 3V 特性[12]。不同类别数据的混杂，使得追溯用户隐私信息泄露的源头更为困难。

---

[1]　收稿日期：

作者介绍：**王树义**，男，1982 年生，博士，讲师，硕士研究生导师。主要研究方向：社交媒体信息分析 。E-mail: nkwshuyi@gmail.com。**吴查科**，男，1991 年生，硕士研究生。主要研究方向：社交媒体信息分析。

1）　本文系国家社科基金青年项目“基于信息价格动态揭示的社交媒体用户隐私保护研究”(项目编号：15CTQ017)的研究成果之一。

二是地理位置隐私保护的责任划分不明晰。以往的研究并未具体详细考察隐私泄露的责任归属，而是主观地判定某一参与主体需要承担责任，进而直接给出解决方案。

科斯定律（Coase Theorem）认为，在不考虑交易成本情况下，多个主体进行责任划分时，避免损失所需要付出的代价最小的一方应被认定为主要责任方[13]。本文依照科斯定律，结合大数据三个维度和“用户”、“开放数据平台”和“监管机构”三个不同主体，制定分析框架。在认定主要责任方和主要泄漏途径的基础上提出针对性的对策。具体而言，本文要解决的问题如下：

(1)在大数据的不同特性维度下，考察地理位置隐私泄露的途径和潜在危害；

(2)在各参与主体中，判定地理位置隐私信息泄露的主要责任方；

(3)探讨主要责任方避免隐私信息泄露的有效对策。

下文我们将在文献回顾的基础上，分析与回应上述问题。

2 文献回顾

本节对隐私信息的泄露责任主体认定以及保护对策等方面的相关文献进行梳理。

2.1 信息泄露责任主体认定

在对于责任主体认定的相关文献中，有人认为运营商应当对信息泄露负责。如 Todd Feinman 认为，运营商在数据泄露事件中因为没有正确管理敏感数据，应该担负主要责任[14]。王利明认为个人信息的大面积泄露的责任问题应当从立法的角度解决，明确运营机构、工作人员与第三方等主体，对侵害个人信息权利所需要承担的责任[15]。一些法律诉讼中，有严重资料违规和数据泄露的公司已经根据各种法律理由被起诉，最终受到严格的法律制裁[16]。也有人将原因归咎于监管机构。吴秋余认为监管和内控机制的不到位，致使一些应用公司对用户的地理位置信息随意进行收集，导致了用户隐私信息泄露[17]。梁启星认为 LBS 位置隐私保护措施的构建需要通过法律、专门委员会等方面进行完善[18]。还有人表示责任在于用户。彭湘蓉认为他者泄露用户信息的前提是对隐私主体个人的了解和掌握，想要消除隐私危机可从隐私信息的源头进行弱化[19]。王娜等人从提升个人的安全素养方面对个人隐私信息保护做出了建议[20]。但是尚未发现有研究者针对开放数据环境下信息泄露的责任划分进行充分而详细地探究。

2.2 隐私信息保护对策类型

各方尝试了从不同角度的许多方法来保护用户地理位置隐私信息。从技术方面来看，目前常用的隐私保护方式包括匿名化和聚合地理位置[21-23]。然而，目前已经有比较成熟的去匿名化算法与工具出现[24]，而且大数据的关联分析技术也使得多角度综合定位成为可能[9,25]，这些新技术使得上述保护用户地理位置隐私信息的手段失去本来应有的效果[7,8]。

从监管方面来看，美国与韩国分别针对地理位置隐私保护出台了《位置隐私保护法案》和《位置信息保护法》。中国自 2016 年开始施行的《地图管理条例》对互联网地图服务单位收集和保护个人信息的义务制定了罚则[26]。但是由于新媒体技术发展日新月异，监管部门即便已经努力应对，相关制度依然不尽完善[27]。

运营商的管理与自我约束方面，Foursquare 已经调整了用户签到功能的 API 数据调用，从最初的记录所有签到位置信息，到目前只有当用户显式指定的时候才会记录地理位置信息[6]。Twitter 也已默认关闭用户的地理位置信息分享[28]。为了让用户可以清楚的看到自己的隐私安全情况，Facebook 推出了一款“隐私检查工具”，以避免用户出现“过度分享”的情况。[29]

用户安全意识培养方面，虽然很多学者做了各种努力[20,30]，但用户依然在轻松愉快且乐此不疲地分享着自己的各种信息[31]。综上所述，目前针对开放数据平台的地理位置信息泄漏问题的责任划定不明确，且提出的各种解决方案效果不佳，本文引用经济学科斯定律界定主要责任

方。

3　研究设计

3.1　研究框架

Jongbin Jung等人通过建立一套简单的决策规则方法，在多个不同大小与复杂性的领域进行研究分析，研究得到的结果与研究采用复杂的回归方法分析出的结果相匹配，他们认为简单规则同样能进行科学决策[32]。本研究在方法设计中采用了这一思想。

我们首先绘制了隐私泄露责任分析框架的初始图。按照初始框架，分别在大数据的三个不同特性下，利用影子分析方法，收集开放数据环境中的地理位置数据，对数据进行可视化操作，进行实例研究。我们根据科斯定律，对避免地理位置隐私泄露所需付出代价最小的主体计1分，其余主体不计分，最后对计分求和。图1为隐私泄露责任分析框架，初始值均为0。

表1　隐私泄露责任分析框架（初始）

相关主体 大数据特性	监管机构	开放数据平台	用户
容量特性	0	0	0
速度特性	0	0	0
种类特性	0	0	0

3.2　研究方法

为了实现研究目标，本文采用的研究方法如下：

（1）数据挖掘。我们使用了开放数据平台所提供的API、Python语言扩展模块tweepy、lxml函数库等对开放数据进行获取与分析。

（2）数据可视化。本文使用Python平台的Bokeh和Google地图API等工具对数据进行可视化分析。

（3）影子分析法。该方法来源于英联邦国家议会的“影子内阁”[33]，目前已经成为竞争情报领域较为流行的一种分析方法[34]，它通过监视某个竞争者或者市场，以深入了解监视对象如何思考、分析和行动。本文使用影子分析法，站在地理位置隐私和窥伺者角度，从开放数据中尝试获得用户隐私数据。

3.2　数据来源

本文分别从以下几个开放数据平台中收集地理位置信息：

（1）社交媒体平台Twitter。https://dev.twitter.com/overview/api

（2）芝加哥市政交通公开数据平台。https://data.cityofchicago.org/browse?category=Transportation

4　容量特性下的信息获取

社交媒体平台每日会产生大量数据，其中大部分包含着地理位置信息，而社交媒体平台有专门的元数据类型专司对用户地理位置信息进行收集。截止到 2016 年 12 月，国际流行社交媒体应用 Twitter 的月活跃用户达 3.13 亿，平均每天发表 5 亿条 Tweets[35]。该社交平平台对外发布了 API 接口，开放部门数据集合，令第三方可以获取到大量的用户地理位置信息。本节便以收集到的 Twitter 用户地理位置数据为例，探讨在容量特征下地理位置隐私泄露的主要责任方。

我们利用 Python 语言扩展模块 tweepy 来收集 Twitter 平台用户发布的 Tweets 数据 。Twitter 不允许用户尝试获取全部 Twitter 数据流，但是开放了 1%的实时随机抽样数据供用户使用，然而对绝大部分研究来说这 1%的数据已过于庞大。因此我们这里做出两个限定：一是我们只收集带有地理位置信息的 Tweets 数据，二是为了避免滥用网络资源，我们只收集 10000 条数据就结束收集过程。

根据收集到的数据，我们发现这些用户都在 Tweets 中透露了自己的地理位置信息。我们采用了 Bokeh 数据可视化工具来标示地理位置信息的用户分布，调用其中的世界地图模型，将收获的 10000 条地理坐标信息“钉”在地图上。获得的结果如图 1 所示。

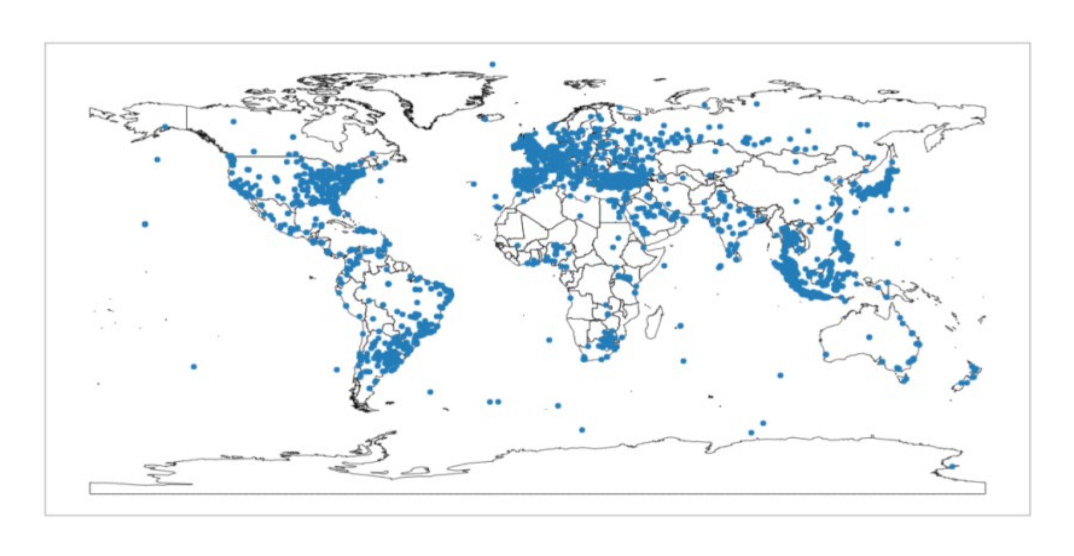


图 1　公开地理位置信息的 Twitter 用户群体分布

从图 1 中我们可以看到，公开了自己地理位置信息的用户分布在世界各地。在我们收集数据的时段里，分布比较稠密的地区主要包括美洲（尤其是美国中东部、巴西南部和阿根廷）、欧洲和东南亚等地。因为时区关系，这一静态图像只展示出了全球一部分用户的所在位置。然而在此案例中，我们可以看到数量庞大的地理位置数据能通过 API 轻易获取，对于主要责任方的分析探讨更显必要。

首先是监管机构，用户在注册 Twitter 时就已同意运营商的服务条款与隐私政策，在两方未违反协议的情况下，监管机构已履行自身职责，不承担用户地理位置隐私信息泄露的责任。对于运营商来说， Twitter 在原始设置当中已经默认关闭了地理位置的分享，需要用户主动主动开启才能进行地理位置的分享。在这个案例中，用户对于地理位置分享是主动并知情的，而运营方并不能干涉用户对于分享功能的使用；用户想要保护隐私信息的安全，只要不去开启分享功能即可。根据科斯定律，“监管机构”和“运营方”不是做出避免地理位置隐私信息泄露所需成本最小的一方，而恰恰是“用户”这个主体所需成本最小。因而在容量特性下，“用户”是地理位置隐私泄露的主要责任方，我们在这里给“用户”计上 1 分。

表 2　隐私泄露责任分析框架

相关主体 大数据特性	监管机构	开放数据平台	用户
容量特性	0	0	1
速度特性	0	0	0
种类特性	0	0	0
总分	0	0	1

5 速度特性下的信息获取

用户在社交媒体平台所生产的数据通常以数据流的形式出现，数据产生速度非常快，如果不能得到及时分析处理便会失去价值[36]。本节研究在大数据速度特性下，在 Twitter 社交平台上某一具体用户的运动轨迹信息可以被实时提取时，主要责任应该由哪一相关主体来承担。

Twitter 会把每一个用户发布的 Tweets 根据时间顺序存储进数据库，在用户点击时可快速生成时间线（根据时间排列的 Tweets）。我们采用被处理过后、存储在数据库的历史数据来跟踪用户动态轨迹，利用 Tweepy 扩展模块的 user_timeline 功能获取指定用户的时间线信息。

从上节中搜集到的 10000 条 Tweets 中,我们随机选择一名用户，根据上一部分获取的信息，得知该用户当前所处位置为印尼。然后编写一段代码，读取该用户时间线信息，并抽取其中全部包含地理位置信息的条目。数据分析的结果显示，该用户最近一段时间活跃在印尼境内。我们还同时获得了经纬度坐标返回列表。积攒了足够的地理位置坐标数据之后，我们依照这些信息在地图上面进行标记。我们调用了 Google 地图 API 中 marker 与 path 功能，描绘了该用户的运动轨迹，如图 2 所示。

从图 2 中可以看出，该用户的活动非常规律，主要活动区域比较小，而且总是在几个固定地点之间穿梭。其中某些路径线非常粗，意味着用户在该路径上面多次往返。根据常识我们推断这几个固定点中包含了用户的住所与工作场所，然而用户被外界清楚了解到这样的活动规律信息则会面临安全风险。

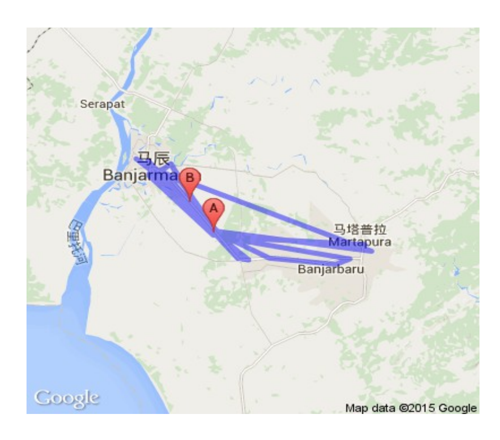


图 2　Twitter 用户运动轨迹可视化

在上一节中，我们已经论证过在用户使用 Twitter 时，监管机构不是用户地理位置隐私泄

露的主要责任方，本节案例中的用户与运营商的主体没有变化，所以我们依然可以推断监管机构在本节中不是主要责任方。对于运营方 Twitter 来说，用户一旦开启了地理位置分享按钮，设置便会默认保存，在下一次撰写 Tweet 时会自动显示位置数据。案例中的用户在分享了一次自己的地理位置后，没有关闭地理位置按钮，也没有做出其他能避免地理位置泄露的保护动作，而是再一次将 Tweet 与地理位置相关联进行了分享。而这些数据都可以实时被他人通过 API 进行查找。根据科斯定律，避免地理位置造成泄露所需要付出最小代价的相关主体依然是用户，计 1 分。

表 3　隐私泄露责任分析框架

相关主体 大数据特性	监管机构	开放数据平台	用户
容量特性	0	0	1
速度特性	0	0	1
种类特性	0	0	0
总分	0	0	2

6　种类特性下的信息获取

互联网中的大数据，包含着种类繁多的信息[37]。即便在 Twitter 等社交媒体应用上关闭了地理位置分享设置，由于大数据的种类特性，用户依然有可能提供背景信息，从而暴露自己的运动轨迹。本节利用影子分析方法，收集用户在开放数据集中的信息，找出在此类情况下的主要责任方。

有的人经常喜欢晒一下自己的行动，将旅途中一些新鲜事物发布分享给自己的好友。例如 Twitter 用户 Eric 发推，说自己在芝加哥 146 路公交车上面，如图 4 所示。





图 3　Twitter 用户在公交车上发布照片信息

Eric 的这一条 Tweet 里面根本没有包含具体的地理位置坐标。在他看来，芝加哥这样的大

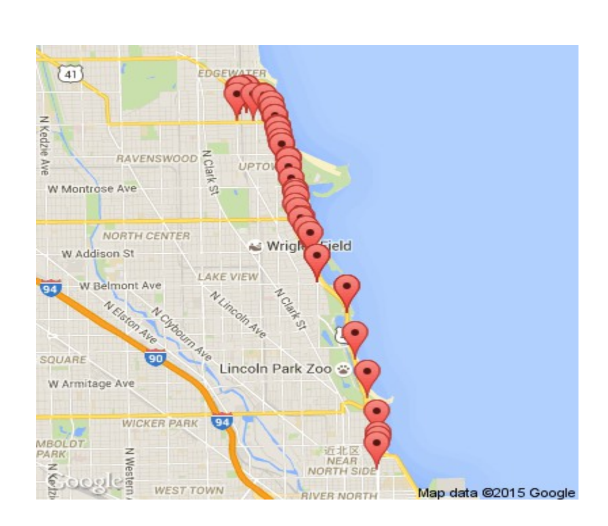
城市公交车有很多，因此这一信息足够宽泛，并不会造成自己位置坐标与活动路径的泄露。然而芝加哥的政府开放数据项目做得非常领先，因此其交通系统（CTA，包含公交和地铁）的运行信息都可以实时查询。

在浏览器中，只需要一条地址指令即可获取某一路线所有车辆的实时位置(http://ctabustracker.com/bustime/map/getBusesForRoute.jsp?route=146.)。输入上一地址，浏览器将反馈给用户一个 XML 文件。这个 XML 文件包含了芝加哥 146 路公交车全部实时运行信息。包含着车辆当前纬度的 lat 字段和经度信息的 lon 字段，还有代表司机工号的 op 字段。即连哪个司机在开哪一辆公交车，以及其实时地理位置信息都一览无余。

开发者可以调用 API，每间隔 60 秒钟查询并且取一次 XML 文件。跟踪时间一个小时之内便可以获取 60 份文件。从这 60 份 XML 文件中，针对每一部车辆可以分别提取经纬度坐标和时间戳信息。我们采用了 lxml 函数库和 xpath 针对 XML 数据进行分析查询，把从 60 份 XML 文件中提取到的车辆路径信息存入一个字典对象，就可以看到在这个时间段里面跑在芝加哥街头的 146 路公交车都有哪些。

我们从取得的数据中任意选择某一辆车，采用 Google Static Maps API 对路径信息进行可视化，将每一个采样的经纬度作为坐标置于图上，观察其运行轨迹。对于代码为 4055 的车辆，运行程序后获得的图像如图 5 所示，该公交车过去一个小时全部行驶轨迹都被清楚标明在了地图上。这样无异于暴露了自己的运动轨迹。

在本节案例中，开放数据平台 Twitter 与用户同样没有违约情况出现，而政府交通系统甚至没有用户的任何数据，我们可以认定监管机构依然不承担任何责任。对“开放数据平台”Twitter 和政府交通系统来说，用户仅仅是在 Twitter 上发布了一条简单的图文信息，甚至没有进行位置分享；而芝加哥交通系统也仅仅的提供了一项实时的交通数据，并没有对用户



地理

图 4　芝加哥编号 4055 的 146 路公交车运行轨迹图

位置信息泄露起到推动作用。所以我们认定两个数据开放平台不是隐私泄露的主要责任方。对于用户来说，在移动社交媒体上发布照片的同时标注详细的车辆信息，是具有地理位置信息泄露隐患的，一旦该用户被别有用心者进行了实时定位，可能会造成财产甚至人身安全都无法保障的后果。本案例中，主要责任方依然是用户这个主体，计 1 分。

表 4　隐私泄露责任分析框架

相关主体 大数据特性	监管机构	开放数据平台	用户
容量特性	0	0	1
速度特性	0	0	1
种类特性	0	0	1
总分	0	0	3

7　讨　论

通过前几节的论述，本研究得出了最终的开放数据环境下用户隐私泄露责任框架表，如表 4 所示，监管机构与开放数据平台得分为 0，用户得分为 3 分，该主体在大数据的 3V 特性下被认为是隐私泄露的主要责任方。

用户在共享地理位置等信息时，即使部分用户已经意识到此类信息行为可能造成隐私泄露，还是会在担忧风险的同时继续分享，Barnes 将这一种现象称之为“隐私悖论”[38]。Bechmann 对 12 个丹麦高中生进行调查过后发现，他们允许运营商随时获取地理位置等隐私数据，即使其中一名同学对此采取谨慎的态度，也还是愿意提供信息[39]。

我们认为有以下两种可能性造成该状况的出现，一是发布地理位置隐私信息可能会为用户带来一定的经济利益。然而对于大部分人而言，分享地理位置不能带来经济收益，而由此可能带来的损失却不好估计。特别是在风险方面，如本文前几节的案例所示，分享地理位置可能带来的财产或人身安全方面的威胁是显而易见的。可以看出，用户进行地理位置分享所可能承受的风险大于可能得到的经济利益，所以利益的可能性不能解释该状况的出现。第二种可能性是由于用户对地理位置信息的价值判断不明，导致信息分享决策失误。误判的原因是用户与开放数据平台之间存在着信息不对称，数据平台掌握着用户大量的信息，并且具备对信息数据充分的商业转化能力，而用户不清楚自己的位置信息最后会被哪些组织机构获取，以及被如何加工利用，从而无法准确地评估隐私风险。同时大数据技术的发展，给用户的位置数据带来了更多泄露途径和方式。所以我们认为是用户与平台之间的信息不对称引起的误判，造成了用户无意识地将地理位置隐私信息进行共享，埋下了泄露的隐患。

要解决用户的信息不对称问题，我们认为要让开放数据平台进行有效准确的提示，让用户充分了解地理位置信息的价值，给其在信息分享决策的过程中有更多的参考依据，以降低决策失误的频率。首先，本文认为地理位置数据的价值需要被量化，运营商可通过用户的位置数据与相关联的数据之间的依赖关系进行位置数据的虚拟价格计算。其次，运营商需要根据虚拟价格计算结果对用户进行风险收益提示，告知用户即将要发布数据的虚拟价格，以及该共享行为可能存在的风险。用户有了提示，对隐私信息进行成本与收益的权衡计算后，能够有效避免因信息不对称而造成的隐私泄露，形成一种良性的信息保护机制。而此举在有效消弭信息部队称的同时，也会增强用户在使用社交媒体时的正向感知，提升用户满意度。从科斯定律的角度来看，这也是一种有效降低交易成本的制度，有利于数据资源向能产生最大价值的一方流动，通过交易的方法实现信息资源的帕累托最优。

而目前主流应用采用的信息价格的计算方法为分批式计算，根据平台上的广告数量去换算成用户的点击流量成本[40]。此法虽有一定可取之处，但是还是不能够做到多种类特性下数据类型的细粒度区分，以及依照实际情况给予用户的个性化输出。如何去改进已有的地理位置信息的虚拟价格揭示手段，进行更加具有个性化的风险提示，是本研究下一步所需要做的工作。

8 结 论

本文采用了经济学中著名的科斯定律，从大数据 3V 特性的不同维度下，对开放数据平台的用户地理位置隐私信息保护进行了综合分析，同时认定了地理位置隐私信息泄露的主要责任方是用户。本文提出通过信息虚拟价格提示的方式，向用户及时透露信息，消除信息不对称，改变用户决策过程，从而确保隐私安全。

本研究的限制在于缺乏个性化的信息价格揭示手段。在进一步研究中，我们会充分寻求社交媒体平台的合作，寻找更丰富的数据来源，以期能找到用户更加个性化风险收益提示，以及信息虚拟价格的计算方法，从而帮助用户在了解地理位置分享行为可能付出的代价后，进行合理决策。

参 考 文 献

[1] Xu L, Jiang C, Wang J, et al. Information Security in Big Data: Privacy and Data Mining[J]. IEEE Access, 2014, 2:1149-1176.

[2] Shadbolt N, O'Hara K, Bernerslee T, et al. Linked Open Government Data: Lessons from Data.gov.uk[J]. Intelligent Systems IEEE, 2012, 27(3):16-24.

[3] Marijn Janssen, Yannis Charalabidis, Anneke Zuiderwijk. Benefits, Adoption Barriers and Myths of Open Data and Open Government[J]. Information Systems Management, 2012, 29(4):258–268.

[4] Shin K G, Ju X, Chen Z, et al. Privacy protection for users of location-based services[J]. IEEE Wireless Communications, 2012, 19(1):30-39.

[5] Mccarthy C. The dark side of geo: PleaseRobMe.com. CNET[EB/OL]. [2016-01-12]. http://www.cnet.com/news/the-dark-side-of-geo-pleaserobme-com/.

[6] Leggio J. Foursquare's privacy loopholes. ZDNet[EB/OL].[2016-01-12]. http://www.zdnet.com/article/foursquares-privacy-loopholes/.

[7] 王璐, 孟小峰. 位置大数据隐私保护研究综述[J]. 软件学报, 2014, 25(4):693-712.

[8] 张学军, 桂小林, 伍忠东. 位置服务隐私保护研究综述[J]. 软件学报, 2015, 26(9):2373-2395.

[9] Smith M, Szongott C, Henne B, et al. Big data privacy issues in public social media[C]// IEEE International Conference on Digital Ecosystems Technologies. IEEE, 2012:1-6.

[10] Wicker S B. The loss of location privacy in the cellular age[J]. Communications of the Acm, 2012, 55(8):60-68.

[11] Jabeur N, Zeadally S, Sayed B. Mobile social networking applications[J]. Communications of the Acm, 2013, 56(3):71-79.

[12] Villars R L, Olofson C W, Eastwood M. Big data: What it is and why you should care[J]. White Paper, IDC, 2011: 14.

[13] Coase R H. The Problem of Social Cost[M]// Classic Papers in Natural Resource Economics. Palgrave Macmillan UK, 2015:837-877.

[14] Todd Feinman. Companies Need to Take Responsibility for Protecting Sensitive User Data. [EB/OL].[2012-02-02]. https://www.entrepreneur.com/article/242355

[15] 王利明. 个人信息保护亟须完善立法[J]. 党政视野, 2016 (11): 45-45.

[16] Advisen. Emerging Cybersecurity Risks for Technology Companies. [EB/OL]. [2010-10-01] http://www.advisenltd.com/2010/10/01/emerging-cybersecurity-risks-technology-companies/

[17] 吴秋余. 谁"偷"了我的支付信息？[N]. 人民日报,2016-11-21(017).

[18] 梁启星. 基于位置服务环境下的位置隐私侵权探析[J]. 重庆邮电大学学报社会科学版, 2013, 25(2):24-29.

[19] 彭湘蓉. 隐私悖论视角下的社交网络隐私安全[J]. 中州学刊, 2016(3):168-172.

[20] 王娜, 许大辰. 移动社交网络中个人信息保护现状的调查与分析--从用户行为习惯视角出发[J]. 情报杂志, 2015(1):185-189.

[21] Ghinita G. Private Queries and Trajectory Anonymization: a Dual Perspective on Location

Privacy[J]. Transactions on Data Privacy, 2009, 2(1):3-19.
[22] Krumm J. A survey of computational location privacy[J]. Personal and Ubiquitous Computing, 2009, 13(6):391-399.
[23] Puttaswamy K P N, Wang S, Steinbauer T, et al. Preserving Location Privacy in Geosocial Applications[J]. IEEE Transactions on Mobile Computing, 2014, 13(1):159-173.
[24] Narayanan A, Shmatikov V. Robust De-anonymization of Large Sparse Datasets[C]// Security and Privacy, 2008. SP 2008. IEEE Symposium on. DBLP, 2008:111-125.
[25] Laurila J. The mobile data challenge: Big data for mobile computing research[C]// Mobile Data Challenge by Nokia Workshop, in conjunction with Int. Conf. on Pervasive Computing. 2012.
[26] 佚名. 《地图管理条例》进一步规范地图出版活动[J]. 中国出版, 2016(1):5-5.
[27] 孟茹. 美国社交媒体平台用户隐私保护的自律与监督机制——以 Facebook 为例[J]. 编辑之友, 2017 (1): 104-112.
[28] Rosen K. Foursquare Updates Privacy Policy to Display Full Names. [EB/OL]. [2016-01-12]. http://mashable.com/2012/12/30/foursquare-privacy/.
[29] Osakwe M. Facebook's Privacy Checkup: What is It and Why is It Important? [EB/OL].[2016-03-02]. http://www.nextadvisor.com/blog/2016/03/02/facebook-privacy-checkup/
[30] 黄启发, 张胜德, 朱建明,等. 基于信息传播规律的社交网络用户隐私保护策略[J]. 情报科学, 2016, V34(5):34-39.
[31] Mylonas A, Kastania A, Gritzalis D. Delegate the smartphone user? Security awareness in smartphone platforms[J]. Computers & Security, 2013, 34(3):47-66.
[32] Jung J, Concannon C, Shroff R, et al. Simple rules for complex decisions[J]. Social Science Electronic Publishing, 2017.
[33] Rothberg H N. Fortifying competitive intelligence systems with shadow teams[J]. Competitive Intelligence Review, 2006, 8(2):3-11.
[34] Fleisher C, Bensoussan B. Business and Competitive Analysis: Effective Application of New and Classic Methods[M]. 2007.
[35] Meg. 40 amazing Twitter stats to inspire your 2017 social strategy[EB/OL]. [2016-12-1].https://www.talkwalker.com/blog/40-amazing-twitter-stats-to-inspire-your-2017-social-strategy.
[36] Fan W, Bifet A. Mining big data:current status, and forecast to the future[J]. Acm Sigkdd Explorations Newsletter, 2013, 14(2):1-5.
[37] Mcafee A, Brynjolfsson E. Big data: the management revolution[J]. Harvard Business Review, 2012, 90(10):60-6, 68, 128.
[38] Barnes S B. A Privacy Paradox: Social networking in the United States[J]. 2006, 11(9).
[39] Bechmann A. Non-Informed Consent Cultures: Privacy Policies and App Contracts on Facebook[J]. Journal of Media Business Studies, 2015, 11(1):21-38.
[40] Hartwig M, Reinhold O, Alt R. Privacy Awareness in Mobile Business: How Mobile OS and Apps Support Transparency in the Use of Personal Data[C]// Bled Econference. 2016.